

USDA PRIVACY IMPACT ASSESSMENT FORM

Project Name:

Geospatial Data Gateway (also called Resource Data Gateway, or just Gateway) – an application in the Natural Resource Information, Inventory, and Assessment IT Investment.

Description of Your Program/Project:

The mission of the Natural Resources Conservation Service (NRCS) is to provide leadership in a partnership effort to help people conserve, maintain, and improve the nation's natural resources and environment. NRCS assists owners of America's private land with conserving their soil, water, and other natural resources. NRCS delivers technical assistance based on sound science and suited to a customer's specific needs.

The Geospatial Data Gateway IT business applications support the conservation planning core mission of NRCS. The Geospatial Data Gateway allows user to identify an area of interest, select available geospatial data for that area, and provides packaging and order fulfillment of geospatial data in support of conservation programs, analyzing and reporting progress, and management applications.

The nature of the NRCS operational environment is a widely distributed operational environment – NRCS provided services in over 3000 offices throughout the US, Caribbean a Pacific Basin – and the complexity of managing natural resource information creates expensive and challenging problems for IT. Unlike more traditional business sectors such as banking or marketing, many of the natural resource business processes have never been automated. The science is often complex and is not well understood. There are considerable differences in the implementation of similar business processes for state to state and office to office. There are few commercially available automated business applications. Application development involves integration of underlying COTS framework software and extensive customization.

The 2002 Farm Bill is changing the way NRCS IT products are developed, managed, delivered, and consumed. In the past the primary users of IT were NRCS employees and to a limited extend conservation districts. The Farm Bill authorized USDA to use Technical Service Providers (TSPs). This authorization is creating a new industry of certified professionals (TSPs) from the private sector, non-profit organizations, and public agencies to provide direct technical assistance and deliver conservation services authorized in the \$3.0 billion in conservation assistance. Technical assistance includes conservation planning and design, layout, installation, and evaluation of approved conservation practices. To be successful and meet the increased demand for providing technical assistance, TSPs like NRCS field offices, will need access to NRCS data and automated conservation planning tools. They will use geospatial technologies like Geographic Information Systems (GIS) and Global Positioning Systems (GPS) to gain efficiencies in planning and installing conservation practices.

DATA IN THE SYSTEM

1. Generally describe the information to be used in the system in each of the following categories: Customer, Employee, and Other.	<i>Customer: General information that can identify the customer and provide means for contacting the customer including name, address, telephone number and email.</i> <i>Employees: same</i> <i>Other: same</i>
2a. What are the sources of the information in the system?	<i>Customer: Data entered directly by the customers.</i> <i>Employees: same</i> <i>Other: same</i>
2b. What USDA files and databases are used? What is the source agency?	<i>None</i>
2c. What Federal Agencies are providing data for use in the system?	<i>USDA – Natural Resources Conservation Service; augmented with specific tabular and spatial information shared by the USDA – Farm Service Agency, CENSUS Bureau, and USGS</i>
2d. What State and Local Agencies are providing data for use in the system?	<i>None</i>
2e. From what other third party sources will data be collected?	<i>No third party services are used.</i>
2f. What information will be collected from the customer/employee?	<i>Customers: For identity purposes – name, address, phone, email</i> <i>Employees & Other: same.</i>
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	<i>No other data is collected.</i>
3b. How will data be checked for completeness?	<i>Data is not checked for completeness.</i>

ACCESS TO THE DATA

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	<i>System managers, developers, and NRCS managers.</i>
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	<i>Users do not have access to databases and data. All access is through application systems that control what information a particular user can view and update. Access is determined by system owners/sponsors.</i>
3. Will users have access to all data on the system or will the user's access be restricted? Explain.	<i>Customers do not have direct access to Gateway customer data. NRCS employee's access is restricted to specific actions by the software applications and to specific data by the eAuth</i>

	<i>security system.</i>
4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	<i>The Gateway application owner identifies very specific access privileges and authority. Each user is restricted to specific actions by the software applications and to specific web screens by the eAuth security system. Developers only have access to the systems they are working on. Database administrators control and grant permissions for access to specific databases as authorized by the business application owners.</i>
5a. Do other systems share data or have access to data in this system? If yes, explain.	<i>No customer data is shared or available to other systems.</i>
5b. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface.	<i>NA</i>
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	<i>No other agencies have access to customer data in the Gateway.</i>
6b. How will the data be used by the agency?	<i>NA</i>
6c. Who is responsible for assuring proper use of the data?	<i>NA</i>

ATTRIBUTES OF THE DATA

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?	<i>Yes</i>
2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	<i>No, all data collection is known to the customer. The aggregate of all data stores does not produce new revelations except in aggregations that produce agency-level statistics on program delivery.</i>
2b. Will the new data be placed in the individual's record (customer or employee)?	<i>NA</i>
2c. Can the system make determinations about customers or employees that would not be possible without the new data?	<i>NA</i>
2d. How will the new data be verified for relevance and accuracy?	<i>NA</i>
3a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	<i>Sensitive information is protected through application and eAuth security.</i>

3b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	<i>Stewardship of the data continues regardless of the distribution or aggregation.</i>
4a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	<i>Data is only accessible through business applications. Customers have no direct access to the data.</i>
4b. What are the potential effects on the due process rights of customers and employees of: <ul style="list-style-type: none"> consolidation and linkage of files and systems; derivation of data accelerated information processing and decision making; use of new technologies. 	<i>Customers and employees have due process rights regardless of the physical structure of a particular database.</i>

MAINTENANCE OF ADMINISTRATIVE CONTROLS

1a. Explain how the system and its use will ensure equitable treatment of customers and employees.	<i>The system is based on agency business processes. Any customer who has access to the Internet receives the same attention from the computer, and is processed under the same automated business rules as any other customer.</i>
2a. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?	<i>The Gateway system is operated at multiple sites. Procedures and process are in place to assure continuance of operations and to assure the integrity of the system.</i>
2b. Explain any possibility of disparate treatment of individuals or groups.	<i>There is nothing inherent to Gateway that would allow any possibility of disparate treatment.</i>
2c. What are the retention periods of data in this system?	<i>There are no defined retention periods for customer data entered into the system. The longevity of the system is not known, but data regularly outlives a particular processing system. Legal requirement for data retention are adhered to, as applicable.</i>
2d. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	<i>Since there is no defined retention period, there are no procedures for eliminating data. At some point the usefulness of the data will be evaluated on a case-by-case basis to determine if it should be retained or not.</i>
2e. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	<i>Data relates to a particular business transaction between the government and the customer for delivery of geospatial data. Business transactions are recorded and concluded, and remain as historic documentation of a completed event. It does not change further over time unless there is a subsequent business transaction conducted.</i>

3a. Is the system using technologies in ways that the USDA has not previously employed (e.g. Caller-ID)?	<i>No</i>
3b. How does the use of this technology affect customer/employee privacy?	<i>NA</i>
4a. Will this system provide the capability to identify, locate, and monitor <u>individuals</u> ? If yes, explain.	<i>No</i>
4b. Will this system provide the capability to identify, locate, and monitor <u>groups of people</u> ? If yes, explain.	<i>No</i>
4c. What controls will be used to prevent unauthorized monitoring?	<i>Security controls are rigorously applied and monitored. The Gateway application is in the process of undergoing a Security Certification and Accreditation process that will identify the risks to unauthorized use and implement a plan to mitigate the risks where possible.</i>
5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.	<i>Notice of Privacy Act System of Records by Owner, Operator or Producer Files (or Volunteer / Employee Files) USDA/NRCS-1</i>
5b. If the system is being modified, will the SOR require amendment or revision? Explain.	<i>NA</i>